PAST | FUSION CELL
PUBLIC AFFAIRS SCIENCE AND TECHNOLOGY

Argonne NATIONAL LABORATORY

PUBLIC SAFETY AND LEGAL IMPLICATIONS OF BANDWIDTH THROTTLING

Bethany Glandorf, Attorney, Collins Legal
Holly Hardin, Co-Director/Communications Analyst, PAST Fusion Cell

INTRODUCTION

Due to communication issues with the Mendocino, CA wildfire, which is now the state's largest wildfire to date, twenty-two states and the District of Columbia, the County of Santa Clara, the Santa Clara Central Fire Protection District, and the California Public Utilities Commission filed a new Brief in support of a consolidated petition challenging the Federal Communications Commission's (FCC's) decision to repeal net neutrality, which restricted service providers from blocking or slowing Internet access or from speeding it up for a higher charge. That Petition is under legal review in the Federal Court of Appeals for the District of Columbia. During a critical time for the emergency response, the Petitioners allege Verizon reduced Santa Clara County's data rates to one two-hundredths of what was usual. Ultimately, Santa Clara County had to subscribe to a higher priced data package to resolve the communications issue (Dwyer, 2018). According to the Santa Clara County Fire Chief Anthony Bowden, as cited in an NPR article on the Mendocino, CA wildfire throttling issue,

Wireless (Wi-Fi) networks only work within the range of a router. With a data plan, subscribers can access the Internet on a phone or tablet even when the user is out of Wi-Fi range. Additionally, according to Verizon's website, access to the Internet on a data plan offers a higher level of security when using the Internet (Verizon, 2015).

The effectiveness of data communication connectivity during high usage times, such as during emergency events when public safety agencies are responding and community members are calling for help, is left up to each public safety agency's relationship with its respective data carrier. It is their responsibility to contact a representative from the carrier to request an increase in data usage. This doesn't always work as intended, as illustrated during the Mendocino Wildfire (Dwyer, 2018). While many public safety agencies are trained for and exercise to respond effectively to emergencies, emergency events can be unpredictable. Determing when enhanced data usage may be needed is not something that can always be planned for. Additionally, public safety agencies may not have an existing relationship with data carriers or may not be able to reach a carrier representative when needed, which was the case in the Mendocino Wildfire.

> "*Dated or stale information regarding the availability or need for resources can slow response times and render them far less effective. Resources could be deployed to the wrong fire, the wrong part of a fire, or fail to be deployed at all,*" Bowden said. "*Even small delays in response translate into devastating effects, including loss of property, and, in some cases, loss of life*" (Dwyer, 2018).

PUBLIC SAFETY IS DEPENDENT ON COMMUNICATIONS

We are a nation dependent on wireless connectivity, especially during times of crisis (Kim & Hastak, 2017). During the 2017 northern California wildfires, a lack of communication and warnings, and limited firefighting resources have largely been debated as major issues (Orsekes & Grad, 2017). Sonoma County was the focus of sharp criticism for failing to use a federal alert system to send emergency alerts and notify cellphones the night of the fire. County officials have said they feared causing a broad panic that would gridlock evacuation routes. Similarly, in Mendocino County, sheriff's officials said they held off evacuation orders until they could decide where it was safe to send fire evacuees (Orsekes & Grad, 2017). Both counties relied on messaging systems to which only a small fraction of residents subscribed, and which failed when towers were affected by the fires. Wireless Emergency Alerts were not used citing it would target too large a geographic area. Rather, officials took to notify residents through alerts such as Nixle, SoCoAlerts and the CodeRED mobile alert app, all of which require residents to sign up and opt in (Gazzar, 2017). However, even opt-in alerting and texting services such as Everbridge and Nixle rely on wireless providers. In its Privacy Policy, Everbridge indicates carriers are not liable for delayed or undelivered messages and carrier data rates may apply (Everbridge Privacy Notice). As recognized lessons learned from previous fires, California state emergency officials responding to the 2017 Thomas Fire decided to send unprecedented cellphone warnings to an estimated 12 million residents in seven Southern California counties (Orsekes & Grad, 2017).

Community members today go directly to the Internet to receive news updates and emergency information (Kim & Hastak, 2017). For example, with access to the Internet, we can now watch disasters unfold before our eyes via the screens of our smartphones and computers. The Internet is an excellent medium for communities to gather life-saving disaster information and experience the impact of a disaster in a shared manner. However, without access to a wireless router, communities must rely on data connectivity to retrieve this information.

Additionally, responding agencies should expect stakeholders will turn to alternative methods of communication during disasters, particularly when emergency service call centers are overloaded or inoperable. For example, during Hurricanes Irma and Harvey, 911 call centers in Houston were overloaded, so residents began posting to Facebook and Twitter asking for assistance. This occurred despite official agencies' messaging efforts to notify residents they should not use social media to request help (Rhodan, 2017). Responding agencies such as the Houston Police Department and the U.S. Coast Guard sent Facebook and Twitter notifications indicating the public should not use social media as it was not being monitored (Ogrysko, 2017). National guidelines that outline how agencies can and should use social media to help federal agencies during disasters, in addition to a national protocol for social media for geolocation and targeting search and rescue, should be considered for future practice.

LEGAL IMPLICATIONS

In response to issues with emergency alert and warning systems and devastating wildland fires in California in 2017, a bill is working its way through the California Legislature, California SB-833, which would mandate the creation of new guidelines for emergency alert and warning systems. The current version of the bill, as of August 20, 2018, specifically finds that "the size and scope of wild land fires in California have grown significantly over the last decade. These disasters have put the lives of millions at risk and the need to alert residents of danger from these unprecedented disasters has never been greater" (SB-833, CA.2018).

The Bill goes on to require that the Office of Emergency Services ("OES") work with telecommunications and media industry groups, city and county agencies, the disability community, appropriate federal agencies, and others to develop guidelines and rules for alerting and warning the public of an emergency. Importantly, the OES is tasked with developing guidelines for the timing of alerts, best practices, training and staffing of alert and warning systems and agencies, and emergency message templates and standard terminology (SB-833, CA.2018).

Developing standard message templates for alerts and warnings, as well as standard operating procedures and decision making guidelines and processes for state and local agencies, is crucial to ensure that the public is timely and adequately notified; If alert messages are more standardized, confusion can be avoided at a most crucial juncture as many members of the public may receive multiple messages and/or alerts on multiple channels such as television, radio, opt-in mobile alert applications, federal, state, or local emergency alert systems, etc.

In 2015 the Federal Communications Commission ("FCC") reclassified broadband Internet access service as a telecommunication service in the **Matter of Protecting and Promoting Open Internet**. In its Executive Summary contained in the *Report and Order on Remand, Declaratory Ruling, and Order*, (FCC 15-24, released March 12, 2015, GN Docket No. 14-28) the Commission stated, "Threats to Internet Openness remain today. The record reflects that broadband providers hold all the tools necessary to deceive consumers, degrade content, or disfavor the content they don't like" (FCC 15-24, released March 12, 2015, GN Docket No. 14-28, p. 4).

The Commission goes on the state, regarding investment and innovation in expanding technology and broadband networks, "with carefully-tailored rules in place that investment can continue to flourish and consumers can continue to enjoy unfettered access to the internet over their mobile broadband connections. … And consumers must be protected, for example, from mobile commercial practices masquerading as "reasonable network management" (FCC 15-24, p. 5).

The 2015 Order banned three specific practices that the Commission found "invariably harm open Internet".

1. Blocking

A person engaged in the provision of broadband Internet access service, insofar as such person is so engaged, shall not block lawful content, applications, services, or non-harmful devices, subject to reasonable network management.

2. Throttling

A person engaged in the provision of broadband Internet access service, insofar as such person is so engaged, shall not impair or degrade lawful Internet traffic on the basis of Internet content, application, or service, or use of non-harmful device, subject to reasonable network management.

3. No Paid Prioritization

A person engaged in the provision of broadband Internet access service, insofar as such person is so engaged, shall not engage in paid prioritization. "Paid Priority" refers to the management of a broadband providers network to directly or indirectly favor some traffic over other traffic, including through the use of techniques such as traffic shaping, prioritization, resource reservation, or other forms of preferential traffic management, either a) in exchange for consideration (monetary or otherwise) from a third party, or b) to benefit an affiliated entity. (FCC 15-24, p.6).

Recognizing that broadband service providers have "both the incentive and the ability to act as gatekeepers" between edge providers and consumers, the Order created a "no unreasonable interference/ disadvantage standard":

Any person engaged in the provision of broadband Internet access service, insofar as such person in so engaged, shall not unreasonably interfere with or disadvantage (i) end users' ability to select, access, and use broadband Internet access service or the lawful internet content, applications, services, or devices of their choice, or (ii) edge providers' ability to make lawful content, applications, services, or devices available to end users. Reasonable network management shall not be considered a violation of this rule. (FCC 15-24, p. 8-9)

Most of the 2015 rules, and the 2010 rules before them, contained an exception for "reasonable network management", defined as:

A network management practice is a practice that has a primarily technical network management justification but does not include other business practices. A network management practice is reasonable if it is primarily used for and tailored to achieving a legitimate network management purpose, taking into account the particular network architecture and technology of the broadband Internet access service. (FCC 15-24, p. 9)

Perhaps presciently, the 2015 Order specifically recognized concerns raised by the practice of mobile providers applying speed reductions to customers using unlimited data plans in ways that effectively force the customer to switch to price plans/service plans with less generous data allowances. The providers (specifically Verizon, in the example provided in the Order and footnotes) attempted to justify the practice as "reasonable network management". However, the Order notes that Verizon did eventually withdraw this change to their unlimited data plans in 2014 – 2015.

On June 11, 2018, the FCC published its *Restoring Internet Freedom Order* which rolled back many of the regulations created in 2010 and 2015 to protect net-neutrality and internet freedom. It effectively allowed broadband providers to engage in the previously prohibited blocking, throttling, and prioritization as long as the providers disclose their network management practices on their own websites or with the FCC. (FCC Initiative-Restoring Internet Freedom at https://www.fcc.gov/restoring-internet-freedom (2018).

In January 2018, prior to the effective date of the 2018 Order, twenty-two states and the Washington D.C. attorney generals filed a Protective Petition for review of the FCC Order, *Restoring Internet Freedom, Declaratory Ruling, Report and Order, and Order*, in the Court of Appeals for the D.C. Circuit. On February 22, 2018, the Mozilla Corporation, a subsidiary of the Mozilla Foundation, whose stated mission is "to ensure an open Internet accessible to all", also filed a Petition for Review of the Restoring Internet Freedom Order in the Court of Appeals for the D.C. Circuit. On August 20, 2018 the Government Petitioners, consisting of twenty-two states, the District of Columbia, the County of Santa Clara, California, Santa Clara County Central Fire Protection District, and the California Public Utilities Commission filed a brief in the consolidated Petition for Review. The brief included an addendum containing the sworn Declaration of Santa Clara County Central Fire Protection District Fire Chief Anthony Bowden. (Mozilla Corp., et. al. v. Federal Communications Commission and the United States of America, D.C. Cir. No. 18-1051(L))(Pl.'s Br.).

In his declaration, Chief Bowden emphasizes his agency's and other emergency responders' reliance on Internet based systems to "provide crucial and time sensitive public safety services". The Chief avers that in August 2018 the Santa Clara County Central Fire Protection District ("County Fire") experienced drastic throttling by its Internet Service Provider ("ISP"), Verizon, during critical response efforts to the massive Mendocino Complex Fire, the largest fire in California state history. Specifically, its Office of Emergency Services Incident Support Unit 5262 ("OES 5262"), the command and control center deployed to the Mendocino Complex Fire, experienced data rates reduced to 1/200, or less, of the previous speeds, severely interfering with the function of OES 5262. County Fire and IT staff attempted communications and negotiations with Verizon to get the throttle lifted on an emergency basis. Chief Bowden states, "Verizon representatives confirmed the throttling, but, rather than restoring [OES 5262] to an essential data transfer speed, [Verizon] indicated that County Fire would have to switch to a new data plan at more than twice the cost, and [Verizon] would only remove the throttling after [County Fire] contacted the [Verizon] department that handles billing and switched to a new data plan. (Declaration of Fire Chief Anthony Bowden). Verizon ultimately did lift the throttling, *after* County Fire subscribed to a new, more expensive plan. (Id. Pl.'s Br., Declaration of Chief Bowden, emphasis added).

Although Verizon released a statement blaming their refusal to lift throttling of County Fire and OES 5262 on a "customer support mistake" and not a net neutrality issue, Santa Clara County Attorney James Williams rejects that argument, stating, "Verizon's throttling has everything to do with net neutrality-it shows that the ISPs will act in their economic interests even at the expense of public safety." (Brodkin, 2018).

Verizon's throttling of the crucial data speeds of emergency responders certainly implicates issues of public safety and potentially impacts the ability of first responders to plan, coordinate, and execute emergency management plans. It may also create unnecessary delays and negatively impacts crucial response times.

WORKS CITED

Brodkin, J. (2018, August 22). Fire dept. rejects Verizon's "customer support mistake" excuse for throttling. ars Technica. Retrieved from: https://arstechnica.com/tech-policy/2018/08/fire-dept-rejects-verizons-customer-support-mistake-excuse-for-throttling/

California SB-833 (2018) Retrieved from: https://leginfo.legislature.ca.gov/faces/billCompareClient.xhtml?bill_id=201720180SB833

Dwyer, C. (2018, August 22). Verizon Throttled Firefighters' Data As Mendocino Wildfire Raged, Fire Chief Says. National Public Radio. Retrieved from: https://www.npr.org/2018/08/22/640815074/verizon-throttled-firefighters-data-as-mendocino-wildfire-raged-fire-chief-says

Everbridge. Privacy Notice. Retrieved from: https://www.everbridge.com/company/legal/privacy-policy

Federal Communications Commission. Restoring Internet Freedom. Retrieved from: https://www.fcc.gov/restoring-internet-freedom

Gazzar, B. (2017, February 26). After devastating wildfires and mudslides, here's how local agencies are improving emergency notifications. Los Angeles Daily Times. Retrieved from: https://www.dailynews.com/2018/02/23/southern-california-agencies-improve-emergency-notifications-in-wake-of-california-wildfires-mudslides/

Kim, J. & and Hastak, M. (2017). Online Human Behaviors on Social Media during Disaster Responses. The Journal of the Naval Postgraduate School for Homeland Defense and Security. Retrieved from https://www.hsdl.org/?abstract&did=805757

Mozilla v. Federal Communications Commission and the United States of America. (2018). Retrieved from. https://ffp4g1ylyit3jdyti1hqcvtb-wpengine.netdna-ssl.com/wp-content/uploads/2018/02/as-filed-Mozilla-Petition-for-Review-WC-Docket-No.-17-108-22Feb2018.pdf

Ogrysko, N. (2017, September 21). Recent Hurricanes Have the Coast Guard Rethinking Social Media's Role in Rescue and Response. Federal News Radio. https://federalnewsradio.com/management/2017/09/recent-hurricanes-have-the-coast-guard-rethinking-social-medias-role-in-rescue-and-response/

Orsekes, B. and Grad, S. (2017, December 16). Essential California: Lessons learned up North helped in battling Southern California infernos. Los Angeles Times. Retrieved from: http://www.latimes.com/newsletters/la-me-ln-essential-california-20171216-story.html

Report and Order on Remand, Declaratory Ruling, and Order. FCC 15-24, released March 12, 2015, GN Docket No. 14-28.

Rhodan, M. (2017, August 30). 'Please Send Help.' Hurricane Harvey Victims Turn to Twitter and Facebook. Time Magazine. http://time.com/4921961/hurricane-harvey-twitter-facebook-social-media/

Verizon. (2015, March 10). What's the difference between WiFi data and cellular data? Retrieved from: https://www.verizonwireless.com/articles/whats-the-difference-between-wifi-data-and-cellular-data

ARGONNE NATIONAL LABORATORY

- U.S. Department of Energy research facility
- Operated by the University of Chicago
- Midwest's largest federally funded R&D facility
- Located in Lemont, IL, about 25 miles (40 km) southwest of Chicago, IL (USA)
- Conducts basic and applied research in dozens of fields
- Unique suite of leading-edge and rare scientific user facilities

CONTACT
National Public Affairs Academy
Argonne National Laboratory
Phone: 630-252-3146
E-mail: npaa@anl.gov
pastfusion.gss.anl.gov

U.S. DEPARTMENT OF ENERGY
Argonne National Laboratory is a U.S. Department of Energy laboratory managed by UChicago Argonne, LLC.